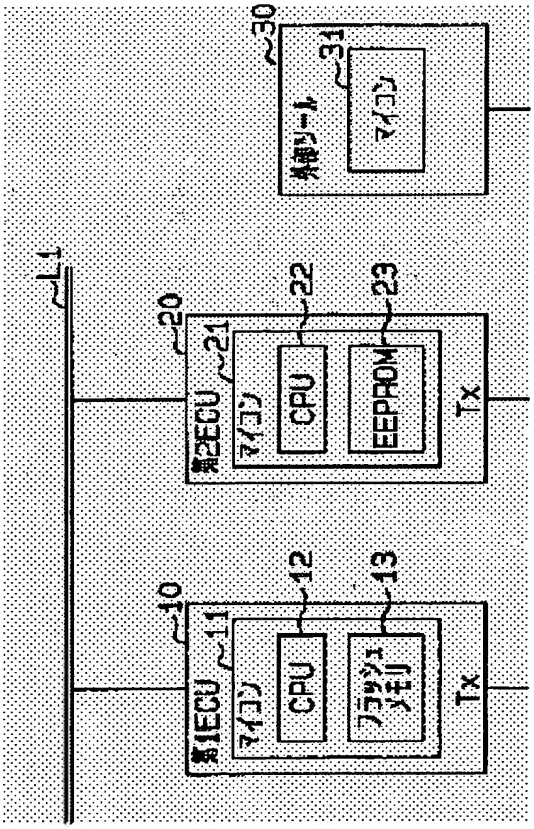
METHOD FOR INSPECTING ON-VEHICLE CONTROL UNIT

Patent number: JP2001202129
Publication date: 2001-07-27
Inventor: NAKAYAMA KIYONARI; KAMIYA KENJI
Applicant: DENSO CORP
Classification:
- international: G05B23/02; F02D45/00; G06F11/10; G06F12/16
- european:
Application number: JP20000012802 20000121
Priority number(s):

Abstract of **JP2001202129**

PROBLEM TO BE SOLVED: To correctly inspect an on-vehicle control unit and to prevent the unit from being illegally modified.

SOLUTION: First and second ECUs 10, 20 are mutually connected so as to be communicated with each other through a multiplex communication line L1 and an external tool 30 is connected to respective ECUs 10, 20 through a serial communication line L2. In the decision of (inspecting) the corresponding/ falseness of the 1st ECU 10, the external tool 30 sends transmission data including a sum value calculation command to respective ECUs 10, 20 through the line L2. The 1st ECU 10 receives the sum value calculation command, calculates the sum value of data stored in a flash memory 13 and transmits the sum value to the 2nd ECU 20 through the line L1. The 2nd ECU 20 compares and decides the received sum value with a true sum value and transmits the decided result to the tool 30 through the line L2. Whether the 1st ECU 10 is a normal ECU or a false ECU is decided on the basis of the decision result.



資料①

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－202129
(P2001－202129A)
(43)公開日　平成13年7月27日(2001.7.27)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
G05B 23/02	302	G05B 23/02	302K	3D026
F02D 45/00	376	F02D 45/00	376F	3G084
G06F 11/10	310	G06F 11/10	310B	5B001
12/16	320	12/16	320B	5B018
// B60R 16/02	665	B60R 16/02	665P	5H223

審査請求 未請求 請求項の数7 OL （全 9 頁） 最終頁に続く

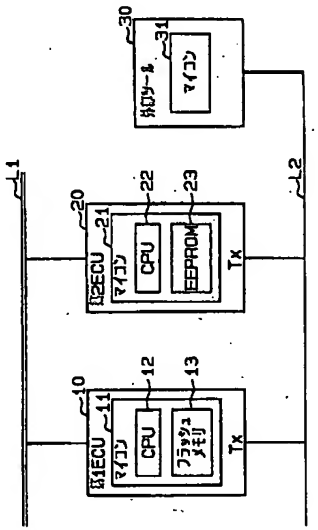
(21)出願番号　特願2000－12802(P2000－12802)
(22)出願日　平成12年1月21日(2000.1.21)

(71)出願人　000004260
株式会社デンソー
愛知県刈谷市昭和町1丁目1番地
(72)発明者　中山　恵也
愛知県刈谷市昭和町1丁目1番地　株式会社デンソー内
(72)発明者　林谷　啓治
愛知県刈谷市昭和町1丁目1番地　株式会社デンソー内
(74)代理人　100058755
弁理士　恩田　博宣　（外1名）

最終頁に続く

(54)【発明の名称】　車載制御ユニットの検査方法

(57)【要約】
【課題】車載制御ユニットを正しく検査し、ひいては不正改造の防止を図る。
【解決手段】第1及び第2ＥＣＵ10，20は多重通信線Ｌ1を介して相互に通信可能に接続され、外部ツール30はシリアル通信線Ｌ2を介して各ＥＣＵ10，20に接続されている。第1ＥＣＵ10の正偽判定（検査）に際し、外部ツール30では先ず、サム値の算出指令を含む送信データをシリアル通信線Ｌ2を介して各ＥＣＵ10，20に送信する。第1ＥＣＵ10では、サム値算出指令を受けてフラッシュメモリ13内のデータのサム値を算出し、その後、そのサム値を多重通信線Ｌ1を介して第2ＥＣＵ20に送信する。第2ＥＣＵ20では、受信したサム値と真のサム値とを比較判定し、その判定結果をシリアル通信線Ｌ2を介して外部ツール30に送信する。この判定結果により、第1ＥＣＵ10が正規ＥＣＵか偽ＥＣＵかが判断される。



【特許請求の範囲】
【請求項1】チェックサムの対象となるメモリを備える第1の制御ユニットと、それとは別の第2の制御ユニットとを備え、前記第1の制御ユニットのメモリについてデータのサム値を求め、該サム値により当該第1の制御ユニットを検査する車載制御ユニットの検査方法において、
サム値の算出指令を外部ツールから第1の制御ユニットへ送信する第1のステップと、
第1の制御ユニット内のメモリのサム値を算出し、該算出したサム値を第2の制御ユニットに送信する第2のステップと、
第2の制御ユニットにおいて受信したサム値を予め用意された真のサム値と比較し、その比較判定の結果から第1の制御ユニットを検査する第3のステップと、
前記検査結果を外部ツールに送信する第4のステップと、
からなることを特徴とする車載制御ユニットの検査方法。
【請求項2】第1の制御ユニット内のメモリは、電気的に書き換え可能な不揮発性メモリである請求項1に記載の車載制御ユニットの検査方法。
【請求項3】前記第2のステップでは、外部ツールが接続される通信線とは異なる別の通信経路を用いて、第1の制御ユニットから第2の制御ユニットへサム値を送信する請求項1又は2に記載の車載制御ユニットの検査方法。
【請求項4】外部ツールは、サム値算出指令の送信後、所定の応答待ち時間以内に受信した受信データを無効とする請求項1～3の何れかに記載の車載制御ユニットの検査方法。
【請求項5】第2の制御ユニットは、外部ツールがサム値算出指令を送信した後、所定の制限時間以内に第1の制御ユニットからサム値が送信されない場合、当該第1の制御ユニットが不正である旨のコード情報を自身の不揮発性メモリに書き込む請求項1～3の何れかに記載の車載制御ユニットの検査方法。
【請求項6】第1の制御ユニットが不正である旨が判定された状態で、第1の制御ユニットから外部ツールへのデータ送信が行われる場合、第2の制御ユニットは、第1の制御ユニットと外部ツールとを結ぶ通信線にダミーデータを送出する請求項1～3の何れかに記載の車載制御ユニットの検査方法。
【請求項7】請求項6に記載の車載制御ユニットの検査方法において、
第2の制御ユニットは、データの送信ポートを論理ハイレベル又はローレベルに保持することでダミーデータを送出する車載制御ユニットの検査方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、車載制御ユニットの検査方法に関するものである。
【0002】
【従来の技術】この種の従来技術として、特開平11－132097号公報の「車両制御用メモリ書き換え装置」がある。同公報の装置は、外部ツールにより電気的に消去及び書き込み可能な制御メモリ（フラッシュメモリ）を搭載したＥＣＵ（車載制御ユニット）を備え、書き換え許可された時にのみ前記制御メモリに対するデータ書き換えが実施される。また、この装置は、制御メモリが記憶するソフトウエア（制御プログラム）が正しいことを検査するものであり、その特徴として、
・予め記憶しておいた制御メモリのサム値（真値）と、ＥＣＵで算出したサム値とを共に表示し、それらを比較することで正偽判定を行う。
・上記サム値の比較は外部ツールの内部で行い、その結果（正偽）のみを返信する。
・イグニッションキースイッチのＯＦＦからＯＮへの切換後にサム値の計算を行う。といった処理を実行する。
【0003】
【発明が解決しようとする課題】上記公報の従来技術では、ＥＣＵで計算したサム値を外部ツールに対してそのまま送信する。そのため、ＥＣＵと外部ツールとの通信データをモニタすることにより、ＥＣＵにより算出した正しいサム値を容易に知り得ることができる。
【0004】また、制御メモリのサム値は、ソフトウエアを書き換えなければ変化しないものであるため、外部チェッカに対して正しいサム値を常に送信するような不正なプログラムを不正改造者が作成し、それをＥＣＵに組み込めば、正規のサム値算出アルゴリズムを知らなくても容易に正規ＥＣＵとしてなりすますことが可能となる。これは、ＥＣＵ側で正偽判定を行う構成でも同様である。すなわち、モニタしたサム値を返答する偽プログラムを不正改造者が作成することにより、不正改造された偽ＥＣＵであっても、外部ツールは正しいサム値（常に同じ）が返答されたと認識し、正しいＥＣＵであると判断してしまう。
【0005】本発明は、上記問題に着目してなされたものであって、その目的とするところは、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる車載制御ユニットの検査方法を提供することである。
【0006】
【課題を解決するための手段】請求項1に記載の車載制御ユニットの検査方法では、（1）サム値の算出指令を外部ツールから第1の制御ユニットへ送信する第1のステップ、（2）第1の制御ユニット内のメモリのサム値を算出し、該算出したサム値を第2の制御ユニットに送信する第2のステップ、（3）第2の制御ユニットにおいて受信したサム値を予め用意された真のサム値と比較

し、その比較判定の結果から第１の制御ユニットを検査する第３のステップ、（４）前記検査結果を外部ツールに送信する第４のステップ、といった各ステップを順に実施する。それ故、仮に正規の制御ユニットが不正改造され、メモリの正しいサム値を外部ツール側に返信できるような不正なプログラムが制御ユニットに組み込まれたとしても、第２の制御ユニットの改造又は置換を併せて実施しなければ、偽の制御ユニットが正規の制御ユニットとしてなりすますことはできない。その結果、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる。

【０００７】上記発明は特に、フラッシュメモリ等、電気的に書き換え可能な不揮発性メモリにて第１の制御ユニット内のメモリが構成される場合に有効である（請求項２）。

【０００８】請求項３に記載の発明では、前記第２のステップにおいて、外部ツールが接続される通信線とは異なる別の通信経路を用いて、第１の制御ユニットから第２の制御ユニットへサム値を送信する。本発明によれば、第１の制御ユニットから発信されるサム値の算出結果が外部ツールで受信されることがないので、外部ツール側で本来必要でないデータが受信され、それが原因で処理が混乱するといった不都合が回避される。

【０００９】請求項４に記載の発明では、外部ツールは、サム値算出指令の送信後、所定の応答待ち時間以内に受信した受信データを無効とする。つまり、外部ツールがサム値算出指令を送信すると、当該外部ツールは本来、上記第２～第４の各ステップが実施される処理時間を経た後、サム値算出指令に応答するデータを受信する。こうした実状にも拘わらず、サム値算出指令の後、直ぐに外部ツールがデータを受信した場合、制御ユニットが不正改造された可能性が高い。それ故、規定に満たない時間で受信したデータを無効化すると共に、制御ユニットが不正改造された旨を判断する。

【００１０】請求項５に記載の発明では、第２の制御ユニットは、外部ツールがサム値算出指令を送信した後、所定の制限時間以内に第１の制御ユニットからサム値が送信されない場合、当該第１の制御ユニットが不正である旨のコード情報を自身（第２の制御ユニット内）の不揮発性メモリに書き込む。かかる場合にも、制御ユニットが不正改造されたことが判定でき、更にその旨を不揮発性メモリに格納することにより、後々の異常診断に役立てることができる。なお、不揮発性メモリに書き込まれたコード情報は、外部ツールからの要求に従い第２の制御ユニットから外部ツールに送信されれば良い。

【００１１】ところで、第２の制御ユニットにより第１の制御ユニットを検査し、その結果を外部ツールに送信する上記構成では、第１の制御ユニットが不正改造されていても、不正改造された当の制御ユニットが自身を正規ＥＣＵであるとする偽データを送信すると、外部ツールは不正改造された制御ユニットを正規なものと誤って判断するおそれがある。

【００１２】そこで、請求項６に記載の発明では、第１の制御ユニットが不正である旨が判定された状態で、第１の制御ユニットから外部ツールへのデータ送信が行われる場合、第２の制御ユニットは、第１の制御ユニットと外部ツールとを結ぶ通信線にダミーデータを送出する。これにより、不正改造された制御ユニットから外部ツールへ向けて偽データが送出したとしても、ダミーデータで前記偽データが破壊（無効化）される。従って、不正改造された制御ユニットを外部ツールが正規なものと判断するといった不都合が解消される。

【００１３】特に、請求項７に記載したように、第２の制御ユニットは、データの送信ポートを論理ハイレベル又はローレベルに保持することでダミーデータを送出すると良く、これにより簡易構成での実現が可能となる。

【００１４】

【発明の実施の形態】（第１の実施の形態）この発明を具体化した本実施の形態では、エンジン制御等を司るＥＣＵにて車載制御ユニットを構成しており、このＥＣＵに対して外部ツールを接続し、当該ＥＣＵの検査やデータの交換等を行うこととしている。以下、その詳細を図面に従って説明する。

【００１５】図１は、制御システムの概略構成を示すブロック図である。本システムでは、第１の制御ユニットとしての第１ＥＣＵ１０と、第２の制御ユニットとしての第２ＥＣＵ２０とを備える。これら第１及び第２ＥＣＵ１０，２０は、多重通信線Ｌ１を介して相互に通信可能に接続されている。第１ＥＣＵ１０は、燃料噴射制御や点火時期制御等、エンジンの主要な制御を受け持つＥＣＵであり、その内部のマイコン１１は、各種制御の中枢をなすＣＰＵ１２、電気的に消去及び書き込み可能なフラッシュメモリ１３、その他図示しないＲＡＭや入出力回路等を備える。

【００１６】また、第２ＥＣＵ２０は、エアバッグ制御やＡＢＳ制御等、補助的な制御を受け持つＥＣＵであり、その内部のマイコン２１は、各種制御の中枢をなすＣＰＵ２２、電源遮断時にも記憶内容を保持するＥＥＰＲＯＭ２３、その他図示しないＲＡＭや入出力回路等を備える。

【００１７】外部ツール３０も同様に、ＣＰＵ、メモリ、入出力回路等からなる周知のマイコン３１を備える。この外部ツール３０は、第１ＥＣＵ１０の正偽判定等の検査や、同ＥＣＵ１０内のフラッシュメモリ１３のデータ書き換えに際し、シリアル通信線Ｌ２を介して第１及び第２ＥＣＵ１０，２０に接続される。これにより、第１及び第２ＥＣＵ１０，２０と外部ツール３０との間でシリアル通信によるデータのやり取りが行われる。

【００１８】第１ＥＣＵ１０の正偽判定（検査）の概要を、図２を用いて説明する。かかる場合、フラッシュメモリ１３内のデータのサム値と既知の正しいサム値とが比較され、両者が一致すれば、第１ＥＣＵ１０が正規なものであると判断される。なお図２では、処理順序を表すため、（１）～（５）の連続番号を付している。

【００１９】先ず始めに、サム値の算出指令を含む送信データをシリアル通信線Ｌ２を介して外部ツール３０から各ＥＣＵ１０，２０に送信する（図の（１））。第１ＥＣＵ１０側では、サム値算出指令を受けてフラッシュメモリ１３内のデータのサム値Ｘｓｕｍを算出し（図の（２））、その後、そのサム値Ｘｓｕｍを多重通信線Ｌ１を介して、すなわち外部ツール３０が接続されるシリアル通信線Ｌ２とは異なる別の通信経路を介して、第２ＥＣＵ２０に送信する（図の（３））。

【００２０】第２ＥＣＵ２０では、受信したサム値Ｘｓｕｍと、予め登録されている真のサム値Ｘｒｅｆとを比較判定し、その判定結果をシリアル通信線Ｌ２を介して外部ツール３０に送信する（図の（４），（５））。また、この第２ＥＣＵ２０では、サム値不一致の場合に第１ＥＣＵ１０が不正改造されたことを意味するダイアグコードを記憶する。

【００２１】そして、前記判定結果がサム値の一致（Ｘｓｕｍ＝Ｘｒｅｆ）を表すものであれば、外部ツール３０において第１ＥＣＵ１０が正規ＥＣＵであると判断し、前記判定結果がサム値の不一致（Ｘｓｕｍ≠Ｘｒｅｆ）を表すものであれば、外部ツール３０において第１ＥＣＵ１０が偽ＥＣＵであると判断する。

【００２２】以下には、外部ツール３０による第１ＥＣＵ１０の正偽判定に際し、各ＥＣＵ１０，２０及び外部ツール３０内の各マイコン１１，２１，３１により実施される処理の流れを図３及び図４のフローチャートに従い説明する。始めに、外部ツール３０の処理の流れを図３のフローチャートで説明する。

【００２３】例えば修理工場等において作業者が外部ツール３０を操作することで図３の処理がスタートし、先ずステップ１０１では、コマンド送信処理によりサム値算出指令を各ＥＣＵ１０，２０に送信する。また、ステップ１０２ではタイマセットを行う。このステップ１０１，１０２が通信前処理に相当する。

【００２４】その後、この外部ツール３０では、コマンド送信に対する第２ＥＣＵ２０からの受信確認を行う。すなわち、タイムアウトしていないことを条件に（ステップ１０３がＮＯ）、ステップ１０４では、前記ステップ１０１のコマンド送信に対する応答を第２ＥＣＵ２０から受信したか否かを判別する。

【００２５】応答が無いままタイムアウトした場合（ステップ１０３がＹＥＳ）、そのままステップ１０７に進む。ステップ１０７では、通信異常に関するダイアグコードを取り出し、その後、ＥＣＵ異常の旨を判断する。なお、ステップ１０３がＹＥＳの場合、ステップ１０１に戻り、コマンド送信を再度実施しても良い。この場合、コマンド再送信の回数を予め制限しておき、例えばタイムアウトが３回繰り返されると、通信異常であると判断してステップ１０７に進む構成としても良い。

【００２６】コマンド送信に対する応答を第２ＥＣＵ２０から受信すると、ステップ１０５に進み、その受信データ内に含まれるサム値の判定結果を取り出す。そして、その判定結果がサム値一致に該当するものであれば、ステップ１０６を肯定判別し、ＥＣＵ正常である旨を判断する。また、前記判定結果がサム値不一致に該当するものであれば、ステップ１０６を否定判別し、ステップ１０７でダイアグコードを取り出し、その後、ＥＣＵ異常の旨を判断する。

【００２７】次に、第１及び第２ＥＣＵ１０，２０の処理の流れを図４のフローチャートに従い説明する。ここで、図４（ａ）は第１ＥＣＵ側１０の処理を示し、図４（ｂ）は第２ＥＣＵ２０側の処理を示す。先ず、図４（ａ）に従い、第１ＥＣＵ１０側の処理の流れを説明する。

【００２８】第１ＥＣＵ１０内のマイコン１１は、先ずステップ２０１において、外部ツール３０よりコマンドを受信したか否かを判別し、ＹＥＳであればステップ２０２に進み、算出式

Ｘｓｕｍ＝ΣＤａｔａ（ｉ）

により、サム値Ｘｓｕｍを算出する。すなわち、フラッシュメモリ１３内の規定されたアドレス領域についてアドレスｉのデータを全て加算し、その和をサム値Ｘｓｕｍとする。その後、ステップ２０３では、前記算出したサム値Ｘｓｕｍを多重通信線Ｌ１を介して第２ＥＣＵ２０に送信し、本処理を一旦終了する。

【００２９】一方、第２ＥＣＵ２０内のマイコン２１は、図４（ｂ）のステップ３０１において、第１ＥＣＵ１０よりサム値Ｘｓｕｍを含むデータを受信したか否かを判別し、ＹＥＳであればステップ３０２に進み、受信データからサム値Ｘｓｕｍ（生データ）を取り出す。

【００３０】その後、ステップ３０３では、予め登録されている真のサム値Ｘｒｅｆを取り出し、続くステップ３０４では、サム値Ｘｓｕｍ（生データ）と真のサム値Ｘｒｅｆとを比較する。

【００３１】両サム値が一致すれば、そのままステップ３０６に進み、サム値の比較結果をシリアル通信線Ｌ２を介して外部ツール３０に対して送信する。この場合、前記図３の処理では、ＥＣＵ正常である旨が判断される。

【００３２】また、両サム値が不一致であれば、ステップ３０５で第１ＥＣＵ１０が不正改造されたことを意味するダイアグコードをＥＥＰＲＯＭ２３に登録した後、ステップ３０６でサム値の比較結果をシリアル通信線Ｌ２を介して外部ツール３０に対して送信する。この場合、外部ツール３０による前記図３の処理では、ＥＥＰ

ＲＯＭ２３に登録したダイアグコードが取り出されると共に、ＥＣＵ異常である旨が判断される。

【００３３】なお本実施の形態では、図３のステップ１０１の処理が本発明の「第１のステップ」に、図４（ａ）のステップ２０２，２０３の処理が「第２のステップ」に、図４（ｂ）のステップ３０４の処理が「第３のステップ」に、図４（ｂ）のステップ３０６の処理が「第４のステップ」に、それぞれ該当する。

【００３４】以上詳述した本実施の形態によれば、以下に示す効果が得られる。つまり、上記ＥＣＵの検査方法によれば、仮に第１ＥＣＵ１０（正規のＥＣＵ）が不正改造され、フラッシュメモリ１３の正しいサム値（算出したサム値Ｘｓｕｍ）を外部ツール３０側に返信できるような不正なプログラムがＥＣＵに組み込まれたとしても、第２ＥＣＵ２０の改造又は置換を併せて実施しなければ、偽のＥＣＵが正規のＥＣＵとしてなりすますことができない。その結果、第１ＥＣＵ１０を正しく検査し、ひいては不正改造の防止を図ることができる。

【００３５】また、外部ツール３０が接続されるシリアル通信線Ｌ２とは異なる別の通信経路（多重通信線Ｌ１）を用いて、第１ＥＣＵ１０から第２ＥＣＵ２０へサム値Ｘｓｕｍを送信するので、サム値Ｘｓｕｍが外部ツール３０で受信されることはない。それ故、外部ツール３０側で本来必要でないデータが受信され、それが原因で処理が混乱するといった不都合が回避される。

【００３６】（第２の実施の形態）次に、本発明における第２の実施の形態を説明する。但し、本実施の形態では、上述した第１の実施の形態と同等であるものは説明を簡略化し、第１の実施の形態との相違点を中心に説明する。

【００３７】上記第１の実施の形態では、第２ＥＣＵ２０でサム値の比較判定が行われ、その判定結果のみがシリアル通信線Ｌ２を介して外部ツール３０に送信されるため、この第２ＥＣＵ２０の代わりに正規ＥＣＵであるとの偽データをシリアル通信線Ｌ２に流すことで、偽のＥＣＵが正規ＥＣＵになりすますことが考えられる。すなわち、図５に示すように、第１ＥＣＵ１０（正規ＥＣＵ）の代わりに偽ＥＣＵ４０が組み込まれた場合、偽ＥＣＵ４０自身が「正規ＥＣＵ」である旨の偽データをシリアル通信線Ｌ２を介して外部ツール３０に送信すると、外部ツール３０は偽ＥＣＵ４０が正規なものであると誤判定するおそれがある。

【００３８】そこで、その対策として本実施の形態では、第１ＥＣＵ１０が不正である旨が判定された場合に、第２ＥＣＵ２０よりシリアル通信線Ｌ２にダミーデータを送出し、偽ＥＣＵが「正規ＥＣＵ」である旨の偽データが通信されることを妨害する。以下、第２ＥＣＵ２０並びに外部ツール３０による監視機能について、詳しく説明する。

【００３９】本実施の形態において、外部ツール３０は、前記図３の処理に代えて図６の処理を実施し、第２ＥＣＵ２０は、前記図４（ｂ）の処理に代えて図７の処理を実施する。但し、各図において変更の無い処理は同じステップ数を付すと共に、重複する説明を簡素化する。なお、第１ＥＣＵ１０の処理は前記図４（ａ）をそのまま流用するため、図示及び説明は省略する。

【００４０】図６において、外部ツール３０は、ステップ１０１，１０２で通信前処理を行い、その後、ステップ１０３，１０４で第２ＥＣＵ２０からの受信確認を行う。このとき、タイムアウトしておらず且つ、コマンド送信に対する応答を第２ＥＣＵ２０から正常に受信すると、ステップ４０１に進む。

【００４１】ステップ４０１では、コマンド送信（サム値算出指令）から所定の応答待ち時間Ｔ１が経過したか否かを判別する。この応答待ち時間Ｔ１は、コマンド送信の後、各ＥＣＵ１０，２０で行われる処理の所要時間を考慮して設定される時間であり、本来は応答データを受信する筈のない時間である。但し、このＴ１は勿論、受信タイムアウトを判定する時間よりも短い時間である。

【００４２】データを正常に受信した時に所定の応答待ち時間Ｔ１が経過していれば、第２ＥＣＵ２０からの受信データが正規データであるとみなし、後続のステップ１０５に進む。そして、受信データ内に含まれるサム値の判定結果により、第１ＥＣＵ１０が正常か異常かを判断する（ステップ１０５～１０７）。

【００４３】また、応答待ち時間Ｔ１前にデータ受信した場合は、受信データが偽データであるとみなして当該データを無効とする。そして、直ぐにステップ１０７に進み、ダイアグコードの取り出し、第１ＥＣＵ１０の異常判定を行う。

【００４４】つまり、サム値算出指令の後、応答待ち時間Ｔ１を待たずに直ぐに外部ツール３０がデータを受信した場合、第１ＥＣＵ１０が不正改造された可能性が高いと言える。それ故、規定に満たない時間で受信したデータを無効化する。

【００４５】一方、図７において、第２ＥＣＵ２０は、外部ツール３０からのコマンド受信の旨を判別すると、ステップ５０１からステップ５０２に進み、タイマセットを行う。

【００４６】その後、コマンド受信からの経過時間が所定の制限時間Ｔ２以内であることを条件に（ステップ５０３がＮＯ）、ステップ５０４では、外部ツール３０からのコマンド送信（サム値算出指令）に応答して第１ＥＣＵ１０からサム値を受信したか否かを判別する。

【００４７】こうした受信確認の処理において、第１ＥＣＵ１０からサム値を受信できないまま、コマンド受信からの経過時間が制限時間Ｔ２を超える場合（ステップ５０３がＹＥＳ）、ステップ５０８に進み、異常ダイアグコードをＥＥＰＲＯＭ２３に登録する。すなわちこの場合、第１ＥＣＵ１０が偽ＥＣＵであるとみなし、不正改造が行われたことを意味するダイアグコードを第２ＥＣＵ２０内のＥＥＰＲＯＭ２３に書き込む。

【００４８】また、制限時間Ｔ２以内にサム値を受信すると、後続のステップ５０５に進む。ステップ５０５～５０７では、受信データに含まれるサム値Ｘｓｕｍと、登録済みの真のサム値Ｘｒｅｆとを取り出すと共に、それら両サム値を比較する。そして、両サム値が一致すれば、ステップ５１１に進み、サム値の比較結果（この場合は正常判定の結果）を外部ツール３０に対して送信する。

【００４９】また、両サム値が不一致であれば、ステップ５０８で異常ダイアグコードをＥＥＰＲＯＭ２３に登録した後、ステップ５０９に進む。ステップ５０９では、所定の受信有効時間Ｔ３（ステップ５１０がＹＥＳの期間）内においてＥＣＵ異常時における通信線モニタ処理を実施する。なお、受信有効時間Ｔ３とは、外部ツール３０が受信データを有効とする時間であって、シリアル通信線Ｌ２上の偽データを、外部ツール３０が正規データとしてとり違える可能性がある時間帯に該当する。

【００５０】通信線モニタ処理に際し、第２ＥＣＵ２０は図８の処理を実施する。すなわち、シリアル通信線Ｌ２をモニタし、第１ＥＣＵ１０から外部ツール３０に対して送信されるコマンドがあるかどうかを判別する（ステップ６０１）。そして、コマンド送信が確認されると、シリアル通信線Ｌ２上のコマンドを無効化すべく、送信ポートＴｘからダミーデータを出力する（ステップ６０２）。なお、簡易構成を実現する上では、送信ポートＴｘを論理ハイレベル又はローレベルに保持することでダミーデータを送出すると良い。

【００５１】通信線モニタ処理をＴ３期間内で継続した後、ステップ５１１では、サム値の比較結果（この場合は異常判定の結果）を外部ツール３０に対して送信し、その後本処理を一旦終了する。

【００５２】ここで、通信線モニタ処理について、図９のタイムチャートを参照してより具体的に説明する。つまり、第１ＥＣＵ１０が偽ＥＣＵに置換され、その偽ＥＣＵの送信ポートＴｘから図示のような偽データが送信される場合、第２ＥＣＵ２０は、自身の送信ポートＴｘを論理ローレベルに保持する。この場合、外部ツール３０では、シリアル通信線Ｌ２を介して受信されるデータに関し、ストップビットを検出できないことからエラー発生であると判定され、結果的に受信データが無効化されることとなる。これにより、偽ＥＣＵが正規ＥＣＵであるようになりすますことが防止できる。

【００５３】なお本実施の形態では、上記第１の実施の形態との違いとして、図７のステップ５０７の処理が「第３のステップ」に、図７のステップ５１１の処理が「第４のステップ」に、それぞれ該当する。

【００５４】以上第２の実施の形態によれば、上記第１の実施の形態における効果に加え、以下の特徴的な効果を奏する。

（イ）外部ツール３０は、サム値算出指令の送信後、所定の応答待ち時間Ｔｉ以内に受信した受信データを無効とするので、第１ＥＣＵ１０が不正改造された旨が好適に判断できる。

【００５５】（ロ）サム値算出指令の後、所定の制限時間Ｔ２以内に第１ＥＣＵ１０からサム値が送信されない場合、第２ＥＣＵ２０は第１ＥＣＵ１０が不正改造されたとみなし、その旨のダイアグコードをＥＥＰＲＯＭ２３に書き込むので、異常判定の履歴が記憶保持できる。また、外部ツール３０からの要求に応じてダイアグコードを取り出すことにより、後々の異常診断に役立てることができる。

【００５６】（ハ）第１ＥＣＵ１０が不正改造された旨が判定された状態で、第１ＥＣＵ１０から外部ツール３０へのデータ送信が行われる場合、第２ＥＣＵ２０はシリアル通信線Ｌ２にダミーデータを送出するので、不正改造されたＥＣＵから外部ツール３０へ向けて偽データが送出したとしても、ダミーデータで前記偽データが破壊（無効化）される。従って、不正改造されたＥＣＵを外部ツール３０が正規なものと誤って判断するといった不都合が解消される。

【００５７】なお本発明は、上記以外に次の形態にて具体化できる。上記各実施の形態では、第１の制御ユニットとして、燃料噴射制御や点火時期制御等、エンジンの主要な制御を受け持つ第１ＥＣＵ１０を設け、第２の制御ユニットとして、エアバッグ制御やＡＢＳ制御等、補助的な制御を受け持つ第２ＥＣＵ２０を設けたが、その構成は任意で良い。要は、少なくとも２つのＥＣＵ（制御ユニット）を備え、検査対象ではない方のＥＣＵによりサム値の比較判定を行う構成であれば良い。

【００５８】上記各実施の形態では、第１及び第２ＥＣＵ１０，２０を多重通信線Ｌ１で接続すると共に、外部ツール３０と各ＥＣＵ１０，２０とをシリアル通信線Ｌ２で接続したが、この通信システムの構成を適宜変更しても良い。要は、サム値算出指令及びサム値比較結果が外部ツール３０で送受信される通信経路と、サム値の算出結果が送信される通信経路とが別々に設けられる構成であればよい。

【図面の簡単な説明】

【図１】発明の実施の形態における制御システムの概略構成を示すブロック図。

【図２】ＥＣＵの正偽判定の様子を示す説明図。

【図３】外部ツールの処理の流れを示すフローチャート。

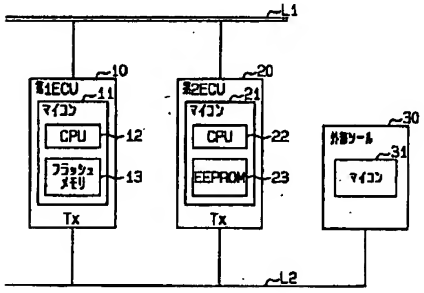
【図４】第１ＥＣＵ及び第２ＥＣＵの処理の流れを示すフローチャート。

【図５】第２の実施の形態の説明のための概略図。

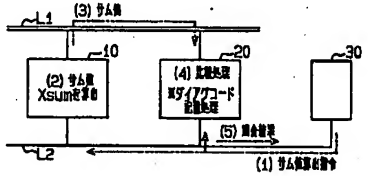
【図６】第２の実施の形態において外部ツールの処理の流れを示すフローチャート。
【図７】第２の実施の形態において第２ＥＣＵの処理の流れを示すフローチャート。
【図８】通信線モニタ処理を示すフローチャート。
【図９】通信線モニタ処理の動作を説明するためのタイムチャート。

【符号の説明】
１０…第１の制御ユニットとしての第１ＥＣＵ、１１…マイコン、１２…ＣＰＵ、１３…フラッシュメモリ、２０…第２の制御ユニットとしての第２ＥＣＵ、２１…マイコン、２２…ＣＰＵ、２３…ＥＥＰＲＯＭ、３０…外部ツール、Ｌ１…多重通信線、Ｌ２…シリアル通信線。

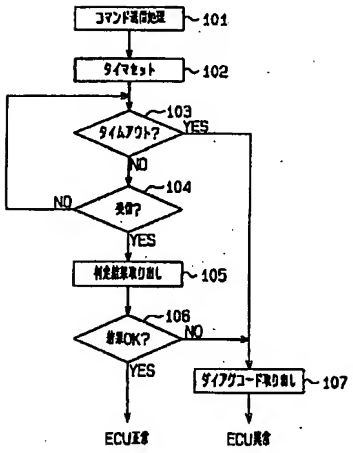
【図１】



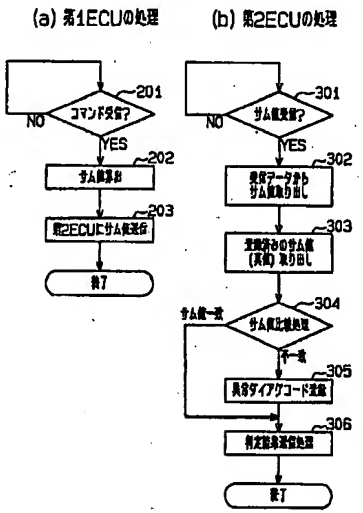
【図２】



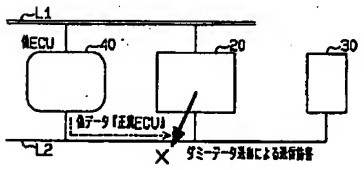
【図３】



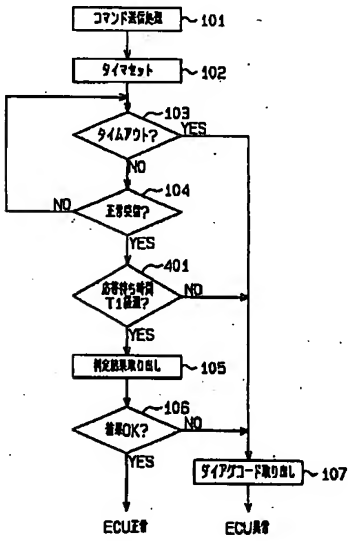
【図４】



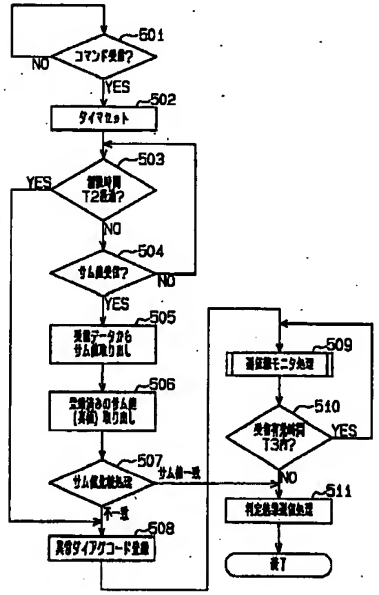
【図５】



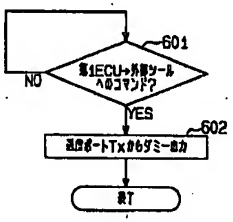
【図６】



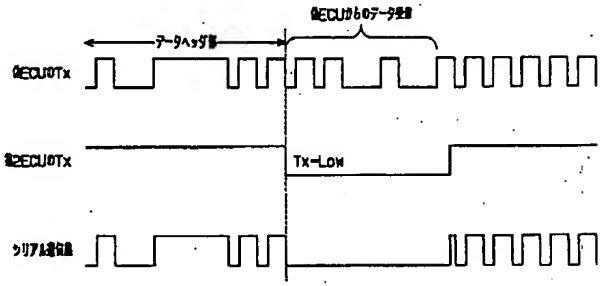
【図７】



【図８】



【図9】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
B60S 5/00		B60S 5/00	9A001

Fターム(参考) 3D026 BA22 BA28
3G084 BA00 DA32 EB06 EB22
5B001 AA14 AB01 AC01 AD03 AE01
5B018 GA03 GA06 GA10 HA13 HA31
JA26 KA12 NA06 RA11 RA12
5H223 AA10 CC08 DD03 EE11 EE19
9A001 BB03 HZ34 JJ77 LL06